Journal of Cybersecurity Education, Research and Practice

Volume 2017 | Number 2 Article 5

December 2017

A toolkit approach to information security awareness and education

Peter Korovessis
Plymouth University, U.K., pkorovessis@acg.edu

Steven Furnell
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, s.furnell@plymouth.ac.uk

Maria Papadaki
Plymouth University, U.K., maria.papadaki@plymouth.ac.uk

Paul Haskell-Dowland
Edith Cowan University, Perth, Australia, p.haskelldowland@ecu.edu.au

A toolkit approach to information security awareness and education

Abstract
In today's business environment where all operations are enabled by technology, information security has become an established discipline as more and more businesses realize its value. The human component has been recognized to have an important role in information security since the only way to reduce security risks is through making employees more information security aware. Towards this goal the research will appreciate the importance of information security awareness by illustrating the need for more effective user training. Further to that it proposes and develops an information security toolkit as a prototype awareness raising initiative. Apart from the elements of toolkit design and development, the research also conducts an assessment of its approach and usability.

Keywords
Information security, information security awareness, information security education, information security toolkit

INTRODUCTION

Security continues to be a major concern not only for companies that provide their services through information technology but also for computer users that use and take advantage of such services. A high level of Internet penetration is reported for both Europe and the US with a growth rate expected at least until 2017 (European Travel Commission, 2014; Pew Research Center, 2014). The World is moving towards a more sophisticated use of technologies such as engaging with social networks and Internet on the move through mobile devices. However, the number of cybercrime incidents has also increased in the last few years (PWC. 2016; Laberis 2016). While companies and organizations significantly invest in the improvement of information security technologies, hackers' interest has shifted by targeting the weakest link: the uneducated computer user (Aloul, 2012). Although all computer users have heard about attacks that can threaten their computers or violate the confidentiality of their data, most of them remain unsure about how to make their computers safe and keep data secure. Similarly, most users are still uninformed about how their system can be compromised due to their insecure behavior. Thus, they continue to visit unsecured websites, respond to phishing e-mails, create weak passwords or store them at non-secure locations or give out sensitive information through exposure to social engineering. This brings into the scene the concept of Information Security Awareness. Therefore, it is important to investigate the potential of raising security awareness within the online population.

Recognizing the importance of information security awareness, this paper examines the need for a more effective user training and proposes an information security awareness toolkit as a prototype awareness raising initiative. As an awareness raising method, the toolkit can be the basis for the general technology user to understand the challenges associated with the secure use of information technology. Additionaly, it will help him assess its current knowledge, identify lacks and weaknesses and acquire the required knowledge to be competent and confident with the use of technology.

THE IMPORTANCE OF INFORMATION SECURITY AWARENESS FOR SOCIETY

Security awareness as a proactive measure, has to do with making end users and employees aware of how to protect personal and organizational information by applying information security practices. According to NIST, information security learning is a continuum which starts with awareness, builds into training and finally evolves into education (National Institute of Standards and Technology (NIST), 1998). Awareness is considered to be the starting point of this continuum and thus is required by all employees. NIST clearly separates awareness from training by defining the purpose of awareness presentations as "simply to focus on security" with an objective to allow individuals recognize IT security concerns and behave accordingly. Awareness is about having knowledge of a situation or fact. In our case, people must have knowledge of security risks and threats before they can be expected to do anything about them. In other words, we cannot expect people to naturally understand existing risks and accordingly react to them, without some form of guidance. The difference between training and awareness lies in the fact that training seeks to teach skills. These skills will allow a person to perform a specific function. On the other hand, awareness seeks to focus an individual's attention on an issue or set of issues. Awareness is a basic necessity, but training is what makes the difference when the real objective is to truly safeguard an organization's sensitive information.

Although the technology to protect information assets is available for many years, yet we continue to hear about serious data losses, large-scale identity theft and the compromise of confidential data. This illustrates the fact that information security is not a technology problem (Lacey, 2009). Given the rising level of breaches (Symantec, 2016), organizations depend upon their users as a key line of defense. It is thus more critical than ever for organizations to raise the level of security awareness. To safeguard a company against all Information Technology (IT) threats requires adequate attention to many aspects of security. Among others, it is important to maintain a high level of employee awareness at all levels and not just among staff whose work is IT-related (Kaspersky Lab, 2013). According to Ernst & Young (2013), companies do not have the skilled resources to support their needs. In fact, only 30% of companies are considered mature or very mature in terms of security awareness, training, and communication. In fact, the establishment of an information security awareness program that will foster the appropriate security culture throughout all levels of the organization, is one of the leading practices that will enable InfoSec improvement (Ernst & Young, 2013). Although Ernst & Young had identified the lack of security awareness among employees since 2013, the situation has not changed significantly. Still, 73% of the surveyed companies are concerned about poor user awareness and behavior around mobile devices. Security awareness and training are considered a high priority by 55% of the respondents. This is considered the third most important priority closely after "Business Continuity" (57%) and "Data leakage/data loss prevention (57%) (Ernst & Young, 2016). As it is important to invest in technology to protect your assets, it is also equally important to invest in the education of employees. Since the company's information security team cannot provide all the necessary security measures for all kinds of threats, an overall enterprise awareness plan is required to cope with the wide variety of incidents, an organization might face. Indeed, such a plan requires the active participation of every employee (Olzak, 2006). It is also realized that an information security awareness program not only adds an extra level of strength in coping with today's threats and attacks but can also be an important component of an organization's business success (Herold, 2005). Through an awareness program, employees know and understand how to maintain the confidentiality of information, and how to handle and secure it appropriately. This ensures (1) compliance with a growing number of laws and regulations regarding forms of training and awareness activities, (2) helps keep customer trust and satisfaction, (3) increase personnel accountability and compliance, and finally (4) increases corporate reputation.

Since end users are using Information and Communications Technology (ICT) services both in their private life and as part of their employment commitments, end user security awareness is one of the most important issues in our society, and everyone should have at least some basic literacy (Anttila et al., 2007). Various reports (ENISA, 2010; CEPIS, 2014) identify that security awareness raising methods should not be focused only on the professional or organizational level but take into serious consideration the home user. Companies and organizations usually spend substantial resources to develop technology and processes that can help safeguard the security of their information assets. Employees at a work setting are in many cases exposed to security training or are protected by special security software and dedicated staff, but this does not apply in the case of home users. Home users are not motivated to take the necessary security precautions to secure their computer and safely use the Internet in a home setting (Anderson and Agarwal, 2010). In fact, infected computers of home users can be the ideal ground for hackers attacking organizations (Li and Siponen, 2011). It will also be of benefit to employers if the embedding and understanding information security concepts are emphasized as early as possible before the threats are encountered in the workplace. In this effort people, organizations and bodies that are already involved in cyber security could help reaching out to end users with information on how to protect themselves against risks. Several practices have been employed in this manner like the cyber security awareness month designed to educate and raise awareness not only to the public and private sector but also to all US citizens (U.S. Department of Homeland Security, 2017). Since the goal of such efforts is to achieve a cultural and behavioral change, home users should be aware on how technical precautions and policies available, usually in a company setting, can also be applied on an individual basis. Such messages and efforts can find a friendly ground on young users and their parents. Academia can play a significant role in these endeavors by engaging educational efforts as early as possible to achieve a stronger effect on users' Internet behavior (CEPIS, 2014).

THE INFORMATION SECURITY TOOLKIT

In addition to numerous studies already available on the subject, there is a significant number of websites that can be identified as valuable resources towards protecting information assets and raising the information security awareness level (e.g. the SANS Institute, WiredSafety.org, StaySafeOnline.org by NCSA, Security Awareness Toolkit by Microsoft Corporation, Stop Think Connect website, the website of the Internet Corporation for Assigned Names and Numbers, etc.). Although there are additional online resources available on the subject, these are representative examples of efforts towards protecting information assets and raising the information security awareness level.

Although a wealth of information is available, even a casual examination of websites reveals that they do not adopt a clear or standardized approach to guide users in relation to security topics. In fact, it can be concluded that the resources available can be an excellent basis for security professionals that are entitled to create awareness materials but can cause confusion to individuals that want to be informed and protected from potential threats. Also, most resources do not offer the ability to test someone's existing knowledge or the knowledge acquired by using the web resources. In many instances, such testing and knowledge verification are desirable before being faced with the task of applying security precautions in a real-world situation. The importance of Information Security knowledge testing has been identified by researchers for more than a decade. For example, Furnell et al. (2002) clearly highlighted the need for a tool that enables individuals to pursue self-paced security training. It also stated that although there are numerous resources available to provide security advice and guidance, they do not offer the ability to test ones understanding in practice. It is highly desirable for individuals to perform such testing before being faced with the task of applying security for real. Still, its lack from many representative sites (as mentioned before) signified that not much had been done in this area. All the above justify the need for a more structured learning approach that could combine all these valuable resources in a more efficient way. Such an approach can make a valuable contribution and may provide a context in which users can learn about security concepts in a more active manner.

In that sense, the research proposes the development of an Information Security Toolkit to help people raise their level of awareness concerning information security. The toolkit will be the basis for general technology users to understand the challenges associated with the secure use of information technology. Not only it can help them assess their current knowledge but also, identify lacks and weaknesses and acquire the required knowledge to be competent and confident users of technology.

Toolkit requirements

The toolkit rationale is mainly derived from the following facts:

- The wide adoption of information technologies over the last ten years, has also changed the profile of end users who use this technology thus bringing great challenges in the area of information security.
- The need for embedding information security in our society.
- The existing awareness raising efforts by representative websites, although they provide a wealth of resources in various formats, they do not follow a structured learning framework thus not guaranteeing coverage or retention of topic knowledge.
- There is a lack of sufficient information security knowledge for higher education students when they enter higher education (Korovessis, 2011).

With these points in mind, the aim of the toolkit is to:

1. Establish a structured approach, so an awareness program adds value to the organization/individual while making a contribution to the field of information security.
2. Provide the means, so existing user knowledge is measured, giving an insight on where security knowledge is lacking through guidance on further knowledge creation.
3. Provide an approach that people can use in a structured and modular fashion so that security knowledge and skills can be built up over time.
4. Include efficient methods of *presentation* and *interactivity*, so participants are more engaged and eventually, an appropriate level of knowledge *retention* is achieved.
5. Provide a web-based system that the user will be able to access anywhere by using minimal information technology resources.

The Art of Knowledge Creation

To develop the toolkit, the knowledge creation process by individuals in organizations was taken into consideration. Individuals create and share knowledge with each other, and thus, knowledge grows through a continuous and dynamic process. A similar model proposed by Nonaka and Takeuchi, called the SECI model (derived from the words Socialization, Externalization, Combination, and Internalization), describes the knowledge creation process (Figure 1), in order to understand the dynamic nature of knowledge creation and to manage such a process effectively (Nonaka and Takeuchi, 1995). Regarding security behavior, tacit knowledge is considered as informal, undocumented or improvised actions performed by personnel as part of their everyday duties on the use of information systems. On the other hand, explicit knowledge is the knowledge that is formal and documented that leaves no room for confusion or doubt. Examples include organizational policies, manuals, and directives. In an organization, the key to knowledge is the conversion of tacit knowledge to explicit knowledge.

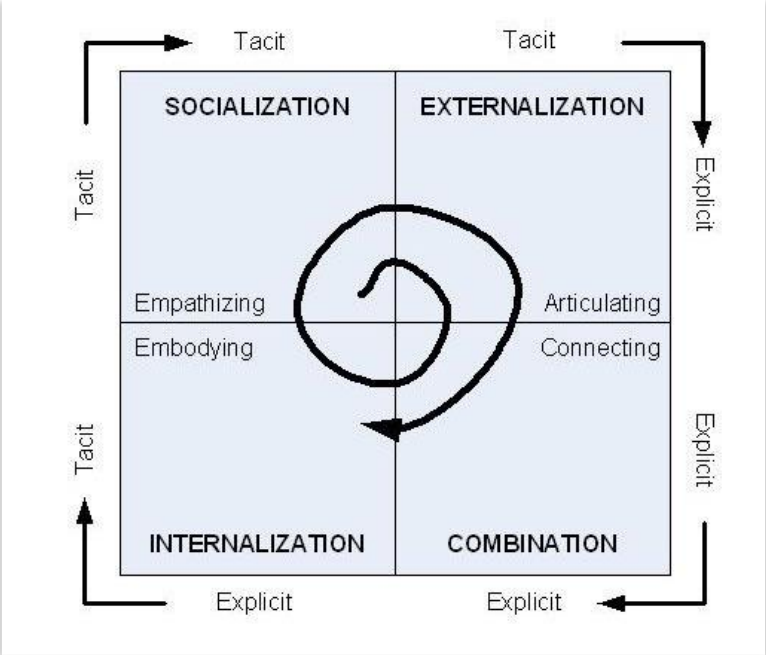


Figure 1: The SECI model by Nonaka and Takeuchi

The theory proposed by Nonaka and Takeuchi is based on four modes that comprise the continuous and dynamic interaction between tacit and explicit knowledge to achieve the creation of knowledge. The modes that identify existing shared informal knowledge and convert it into new formal knowledge are as follows:

- Individuals among a group share tacit knowledge.
- Tacit knowledge becomes formal (explicit) through the formulation and dissemination of appropriate policies.
- Explicit knowledge is transferred to the individual. In this process, individuals absorb explicit knowledge and convert it into tacit knowledge. This can be achieved through simulations and/or training activities.

The cycle then starts again from stage 1 in an infinite loop.

This work can be used to explain the process of a successful security awareness raising effort. The learning path in an organization and the four cyclical stages described above can be used to explain how awareness training can lead to appropriate security behavior. The development of the information security skills toolkit is based on this model of knowledge creation.

Toolkit Development

In developing the toolkit, the four modes theory explained above is put into context as follows (Figure 2):

1. Users undergo information security pre-testing in order for their security level to be measured and appropriate training (if needed) to be proposed. At this stage, the tacit knowledge of the individual is measured.
2. Users undergo security awareness training on areas that weaknesses have been identified into (1). This will be in the form of security awareness material where users will be introduced to correct and incorrect security behaviors. At this stage, the security message is made explicit to the users.
3. Since explicit knowledge needs to be made tacit to the users, after the material has been presented, users take a short test to measure to what extend the message has been internalized.
4. The actual behavior of participants is measured to examine whether their security behavior has changed because of their exposure to the toolkit.

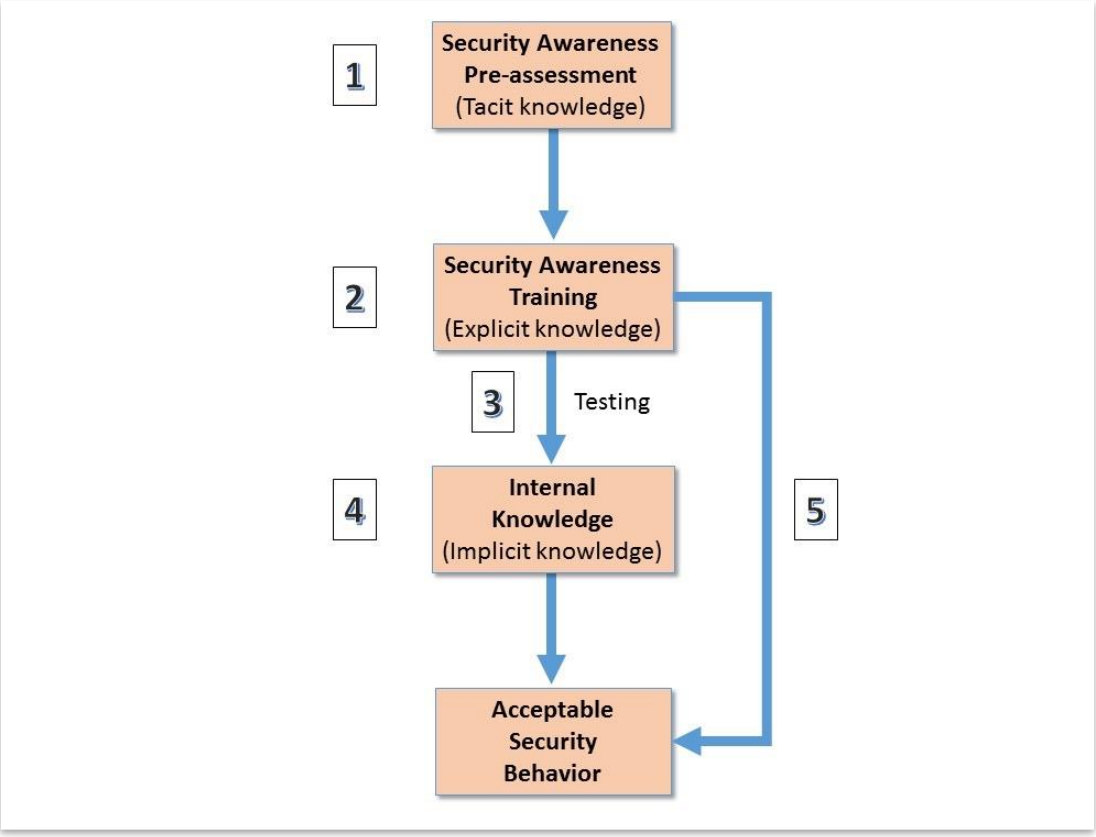


Figure 2: Application of Nonaka's and Takeuchi's theoretical model in the security toolkit.

The toolkit tries to achieve the most effective learning outcome. More specifically it presents different information security concepts through the use of various audio visual means (e.g. text, graphics, and hyperlinks) (Karjalainen et al., 2013). The learner's progress is monitored at the end of each unit of the toolkit. The toolkit will also emphasize why there is a need for compliance with information security procedures by using meaningful examples regarding threats to information assets (Puhakainen and Siponen, 2010).

The toolkit is based on the asynchronous model of learning, allowing the participants to complete the whole or parts of the toolkit at their own pace. The web capability of an HTML5 enabled learning management system can be used as a form of delivery. To enhance learner's skills at areas where real practice is required, the toolkit will be complemented by appropriate simulations to ensure that a change in learner's behaviors is positively achieved.

Toolkit Design

The toolkit will is comprised of the following components:

1. The assessments repository which will include all databases that will store quiz questions to be used in:
   a. The pre-assessment stage of the toolkit where existing knowledge of the participant will be assessed.
   b. The post assessment stage of the toolkit where learning modules have been completed and participant's acquired knowledge should be assessed.
2. The learning unit(s) component which consists of:
   a. The front-end unit which is the actual presentation of the eLearning component of the toolkit accessible through the web.
   b. The back-end unit which contains the actual design and content of each learning module and can be used by toolkit administrators to add/remove or customize content packages based on information security learning materials.
3. The users component which consists of:
   a. End-user who use the toolkit to assess their existing knowledge through the assessment stages and raise their awareness level through the main eLearning components.
   b. Toolkit administrators who are responsible for managing module content and assessment repositories.
4. The user profile database which will contain the personal information of participants (e.g. name, the date they started their engagement with the toolkit, educational background, preliminary IT knowledge), along with toolkit modules completed and assessment results.

From an information systems perspective, the toolkit development is based on the ADDIE (Analysis, Design, Development, Implementation and Evaluation) model. Although many critics of this model argue that it is too linear and inflexible, it remains the most popular model among instructional designers, and most of the current instructional design models are variations of the ADDIE instructional design model. In the ADDIE model, each step has an outcome that "feeds" into the subsequent step in a recursive and continuous process provided that there are updates on the learning materials (Forest, 2014).

Toolkit Implementation

The toolkit was developed having in mind a method of delivery where participants learn at their own pace. For that reason, there was an effort for the learner to control and interact with the learning process as much as possible through continuous feedback regarding the knowledge transfer process. Also, the structuring and presentation of the toolkit around key aspects of baseline security knowledge, will allow them to approach the task in a modular manner. In accordance to Alessi and Trollip's (2000) approach to methods and development of eLearning, the following four activities were used in constructing the toolkit components:

(1) Presentation of Information: although the material presented by the toolkit cannot be considered new for the everyday user, it was found necessary that some presentation of even basic information security concepts to take place.
(2) Learner guidance: through interactivity the toolkit supports the learning process through suggestions and hints.
(3) Practice: possibility for the learner to practice complex tasks.
(4) Assessing Learning: evaluate to what extent learning has been achieved.

What had to be considered though when developing the toolkit was what IT security topics should the general population be aware of, and how these topics should be presented. Publicly available information security surveys, e-mail advisories, IT security related websites, periodicals and information security surveys were used as sources for determining the toolkit material.

In determining what areas and specific topics the e-learning part of the toolkit should include, consideration was given to the NIST guidance. NIST indicates that an information security program should be focused on all the end users within an organization (National Institute of Standards and Technology (NIST), 2003). Also, all individuals who use computer technology or products similar to it, must know IT security basics and be able to apply them, regardless of their profession or job responsibilities (National Institute of Standards and Technology (NIST), 1998). In addition, NIST SP 800-50 suggests 27 information security awareness topics (including password usage and management, protection from malicious code, e-mail and attachments, guidelines on using the web, data backup and restore, social engineering and others) that should be included in any developed security awareness material addressed to all users in an organization (National Institute of Standards and Technology (NIST), 2003). This is also in accordance with other key themes based upon different sources, as is explained later in this research and summarized in Table 1 (sources from ISO/IEC 27002:2013, ENISA, ITGI, EDUCAUSE, and HEISC).

Extra effort was made to introduce security topics through a series of real-life and everyday user experiences and examples. Through these examples, the user exposed to the toolkit had the opportunity to either practice common everyday security concerns (e.g. checking the strength of his/her chose password) or identify other usual security threats like phishing attack examples and social engineering attack procedures.

The toolkit consists of the following parts:

- Pre-assessment,
- Main e-learning unit,
- Post-assessment.

The objective of the pre-assessment unit is to determine the participant's knowledge on specific information security topics and determine whether additional training is needed. Pre-assessment takes place in the form of multiple choice questions which the user should answer. In this prototype model of the pre-assessment unit (Figure 3), two information security areas are covered: (1) Introduction to information security concepts where the participant's knowledge on general information security issues is examined and (2) Human Aspects of Information Security where the objective of the assessment is to examine the participant's knowledge concerning security risks that can arise by poor user choices. The objectives of both pre-assessment units are displayed on the users' screen along with the total number of questions the user will be examined on. At the end of each area examined, a pass or fail score is presented to the participant, and they have the chance to review each answer given and determine the correct answer. A summary is presented at the end of the pre-assessment unit. Upon completion of each pre-assessment unit, the user profile database is updated with the result of each pre-assessment.

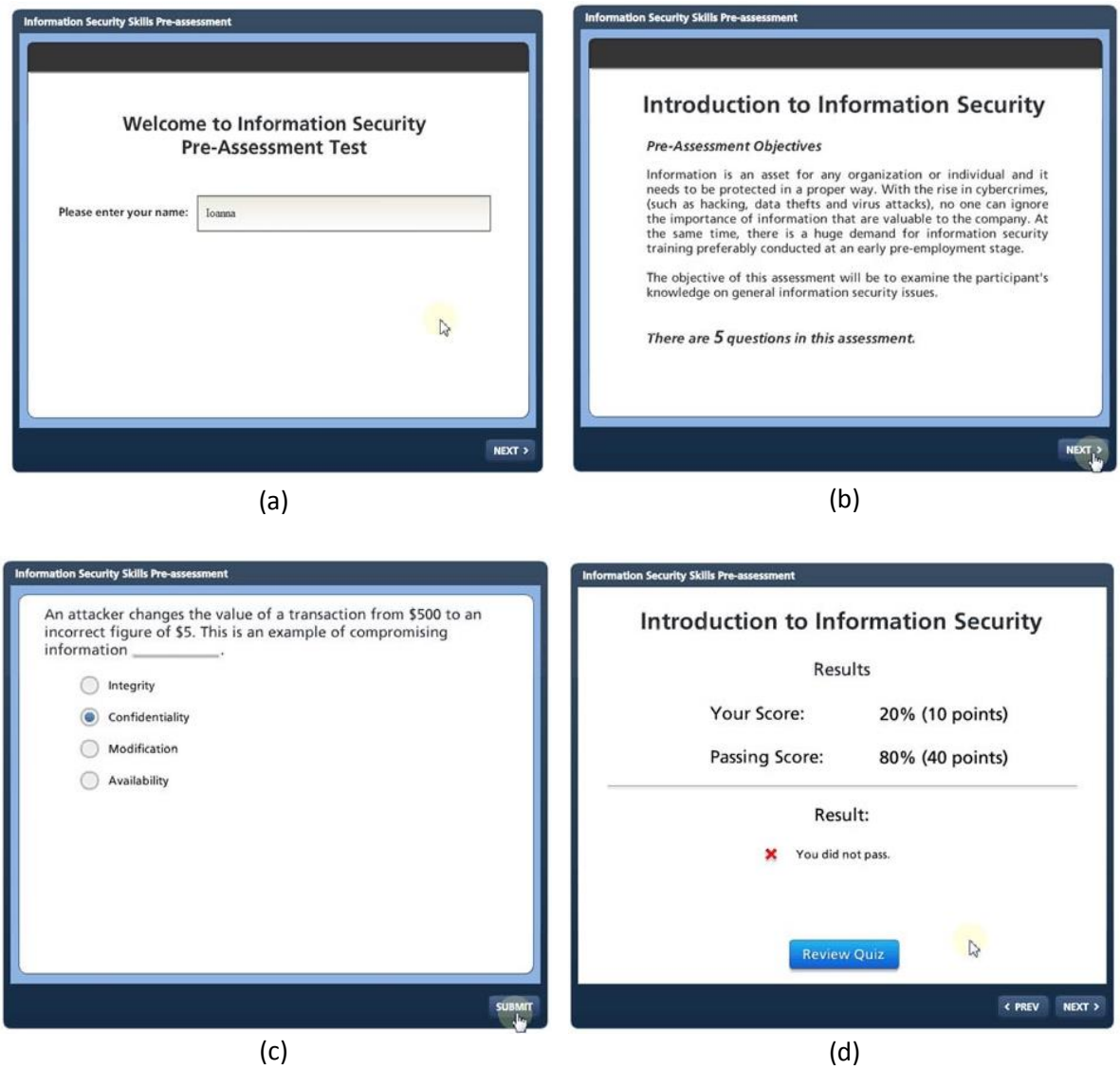
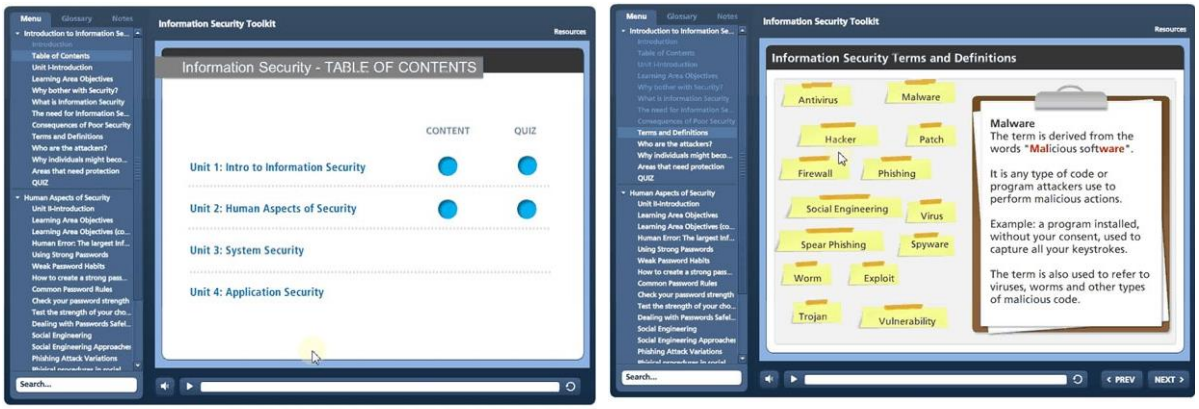


Figure 3: Pre-assessment unit (a) introductory screen, (b) unit objectives, (c) question screen and (d) results screen

The aim of the main e-learning unit, that normally follows the pre-assessment unit, is to introduce participants with essential everyday information security skills and at the same time help those participants in protecting their computers, mobile devices, and data from attacks. It is designed in a way to provide an interactive learning experience to the participant and all that is required to follow it, is a basic working knowledge of computers. In this prototype model of the e-learning unit, two information security areas are covered (1) Introduction to information security concepts and (2) Human Aspects of Information Security (Figure 4). At the end of each unit, the user is returned to the main navigation screen which indicates what part of the e-learning unit has been completed. At that point, the user can take a post-assessment quiz in the form of multiple choice questions so as to assess the level of knowledge that he has gained from the previously covered e-learning part. At the end of the post-assessment quiz, a pass or fail score is presented to the participant, and also has the chance to review each answer given and determine the correct answer. While the participant progresses with each e-learning unit, the user profile database is regularly updated to include module completion progress along with the results of the post-assessment quiz thus allowing meaningful comparisons of achieved knowledge through toolkit engagement.



(a) (b)

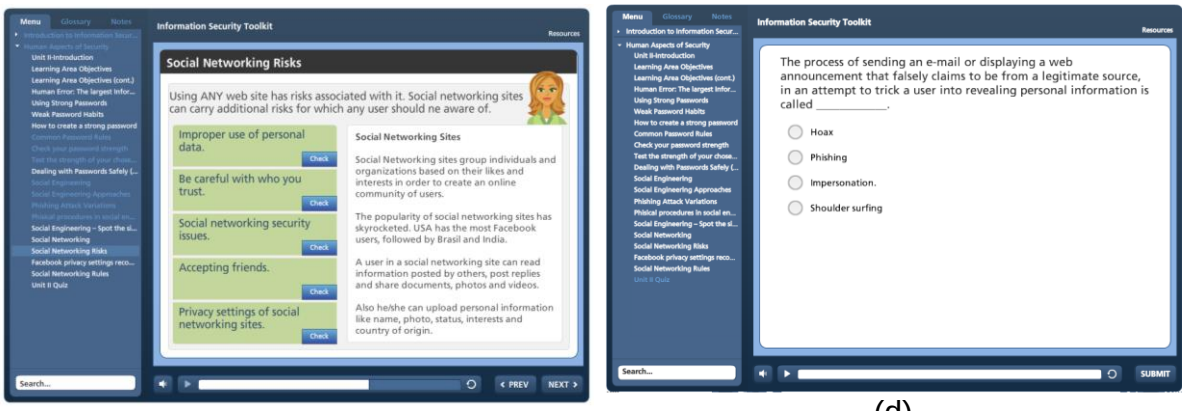


Figure 4: Main e-learning unit (a) introduction screen, (b) sample content screen, (c) sample content and (d) post-assessment screen.

The toolkit was developed as a web-based application to enable easy accessibility for users.

Toolkit Content Areas

In determining the content areas that the toolkit should contain, several sources were examined and analyzed to reach relevant topics that will help raise the level of awareness. The topics were initially determined taking into consideration key Information Security themes, and these were checked for validity and common areas against the following sources:

- ISO/IEC 27002:2013: resources related to the standard on how to manage information security in an organization. Security awareness topics include general concepts about information security and its importance, the human factor, physical security, password use and guidelines, Internet use, e-mail use, etc. (International Organization for Standardization (ISO), 2013).
- ENISA: guidelines on how to raise information security awareness. According to the report, topics like e-mail and electronic communication, passwords, security updates, and patches are important not only to businesses but also to individuals (ENISA, 2007; ENISA, 2010). More specifically the following security areas are important for staff to understand:
    - Human aspects of security (Passwords, social engineering, social networking),
    - System security (Malware, system defenses, and recovery).
    - Application security (use of internet, risks, and defenses).
    - Mobile device security (mobile device threats, attacks, and defenses).
    - Workplace and physical security (Out of the office security, clear desk policy, incident reporting).
- NIST SP 800-50: the National Institute of Standards and Technology guidelines on how to build an information security awareness and training program.
- IT Governance Institute: a comprehensive set of resources that organizations need to adopt as a foundation for good security practices. According to COBIT Security Baseline (ITGI, 2007), home users can be exposed to information security risks mainly due to:
    - Using the Internet without being aware of the dangers associated with it.
    - Installing software from untrusted sources that may contain security weaknesses.
    - Using out-of-date operating systems, security software and application software.
    - Being exposed to attacks from viruses, spyware, spam and phishing that may result to information and identity theft.
- EDUCAUSE and HEISC: resources publicly available as part of the National Cyber Security Awareness Month organized by EDUCAUSE and the Internet2 Higher Education Information Security Council. Through a series of posters, short videos, and training videos, identified topics are around themes like cloud security, antivirus, the importance of backups, Internet security, passwords and workplace security.

The following table maps different information security themes and how they relate to various information security sources.

		Sources					
Key Theme	**Area**	**ENISA**	**NIST 800-50**	**Plessis & von Solms**	**ISO 27002:2013**	**EDUCAUSE & HEISC**	**IT Governance Institute**
General Information Security concepts / InfoSec Importance	Introduction to Information Security	✓	✓	✓	✓		✓
Email and electronic communications	Human Aspects of Security	✓	✓		✓	✓	✓
Physical security / Physical access / Access Control	Workplace Security	✓	✓		✓		✓
Passwords usage and management	Human Aspects of Security	✓	✓		✓	✓	✓
Internet security	Application Security	✓	✓		✓		✓
Viruses	System Security	✓	✓	✓	✓	✓	
Software licensing / Allowed / Supported software	Workplace Security	✓	✓				✓
Security Incident reporting	Workplace Security	✓	✓		✓		✓
Security updates and patches	System Security	✓	✓		✓	✓	✓
Mobile devices / Handhelp device security / Laptop security / Encryption	Mobile Device Security	✓	✓			✓	✓
Out of office security	Mobile Device Security	✓	✓		✓	✓	✓
Personal use of corporate equipment	Workplace Security	✓	✓				✓
Phishing	Human Aspects of Security	✓				✓	✓
Clear desk policy	Workplace Security	✓			✓		✓
Instant messaging	Human Aspects of Security	✓					
Shoulder Surfing	Human Aspects of Security		✓				✓
Policies	Workplace Security		✓	✓	✓		✓
Social Engineering	Human Aspects of Security		✓	✓		✓	✓
Web Usage	Application Security		✓		✓	✓	✓
Data Backups	System Security/Workplace Security		✓				✓
Individual accountability	Workplace Security		✓	✓	✓	✓	✓

Table 1: Information Security key themes according to different sources

Based on the above considerations, the topics/units selected for inclusion in the e-Learning units are the following:

Unit I: Introduction to Information Security

Unit II: Human Aspects of Security

Unit III: System Security

Unit IV: Application Security

Unit V: Mobile Device Security

Unit VI: Workplace Security

Without taking into consideration the existing knowledge of users, all units are expected to play a specific vital role in an effort to raise information security awareness. Unit I – Introduction to Information Security is considered an excellent starting point for any user since it defines the concept of information security and relates it to the protection of valuable assets against unavailability, loss or damage. This unit sets the necessary background and framework for the topics that will follow in the toolkit. The rest of the units are considered of equal importance and based on the existing knowledge of the user may be completed in any particular order although following the prescribed order is strongly recommended.

ASSESSMENT OF SECURITY TOOLKIT APPROACH AND USABILITY

An information security awareness program is considered effective if it can establish the appropriate knowledge and influence the attitude and behavior of the participants towards positive changes in their security culture. To make sure that an awareness program has reached its objectives, appropriate measures need to be in place. Kruger and Kearney (2006) in their study give an example of the development of a measurement model for information security awareness. In this model, changes in security behavior were monitored based on three dimensions: (1) what the employee knows (knowledge), (2) what the employee thinks (attitude) and (3) what the employee does (behavior). These dimensions were subdivided into further areas like keeping passwords and personal identification numbers secret, using the Internet and email in an appropriately safe manner and using mobile equipment carefully.

To provide a complete insight of the effectiveness of awareness raising methods, quantitative data needs to be combined with qualitative data for determining whether the desired effects have been achieved regarding user behavior. Since information security lies in the overlap of attitudes, knowledge, and behaviors, there are a variety of tools and methods that can be used to collect such qualitative data. According to Davis (2008), the most effective methods are summarized in Table 2:

Attitudes	**Knowledge**	**Behaviours**
Surveys	Assessment Tests	Behavioural Measures
Interviews		Surveys
Focus Groups		Interviews
		Focus Groups

Table 2: Most effective methods for measuring the effectiveness of awareness raising methods.

The following methods were used for measuring the toolkit usability:

- Focus groups as a form of group interview. The focus group will not only collect data from several people at the same time but will also encourage interaction and exchange of ideas that will help in exploring people's knowledge and experiences.
- Surveys as a tool for collecting quantitative data from a larger group of individuals.
- Short semi-structured interviews to explore the views, experiences, beliefs and/or motivations of a small group of people on a specific matter or topic.

It should be noted here that surveys, interviews, and focus groups are the generally accepted methods for measuring attitudes. Still, there might be a gap between what people *say* they do, and what they *actually* do, especially in the case of Information Security. For example, people claim to understand how strong passwords are created and how frequently they should be changed, but in practice, they often behave differently. In any case, these methods are considered effective for measuring the toolkit usability, because the assessment at this stage is to measure the users' impression regarding the appropriateness/suitability of the tool rather than the impact that it may have upon their behaviour.

The purpose of the assessment was to evaluate the usability of the toolkit as a platform/approach using the following representative *focus* groups:

- A group of first-year college students. The rationale for choosing this group was to investigate what effect the toolkit would have on students that were at the beginning of their college career, who may have had very little or no information security experience.
- A group of students towards graduation. It is generally accepted that students at this stage are more mature, mainly because of their studies and their proximity to joining the workforce. However, this maturity

does not necessarily include security awareness as a component at least for those that do not have information technology as a core part of their studies. Choosing such a group to investigate what effect the toolkit will have on graduating students, will provide a valuable insight concerning their everyday attitudes towards information security.

- A group of people that hold administrative positions. This group was included to investigate if exposure to the toolkit would have an effect on their level of security behavior. Although sophisticated technology and technical countermeasures are present at most companies to protect information and computer systems, humans are frequently cited as one of the weakest links in the information security chain (Lacey, 2009; McIlwraith, A. 2006). An appropriate security awareness level for the general workforce is crucial for the success of any information security effort.

For all focus group participants, the following procedure was followed:

- Participants completed a short questionnaire concerning their information security experience.
- Participants fully completed the awareness-raising provided by the toolkit.
- A discussion on their experience followed.

In addition to the above focus groups, the toolkit concept and usability was assessed by using two additional groups of individuals:

- A group of individuals from institutions of higher education who are involved in the learning process from various positions (e.g. Librarians, technology specialists, academics, teaching and learning department staff, course designers, etc.). This assessment was done by exposing this group of individuals to the toolkit, and their opinions were measured and analyzed through a survey.
- A group that includes experts in the field, like people closely related to the IT function, IT managers/administrations and information security experts. Similarly, as the previous group, this group of experts was exposed to the toolkit through a survey, and their opinions were measured and analyzed. In addition, short interviews were conducted.

The Student groups toolkit assessment

From the discussion that followed with both student groups, most of them expressed the opinion that such a subject would be best presented and covered using only e-learning means of delivery.

Concerning the toolkit usability, the participants agreed that it was easy to use, useful and had a positive influence on them in adopting and using it further as an awareness raising system. An addition that one of the participants suggested was the creation of a "unit preparation" module (he actually mentioned that could be named "how to use this system") that would demonstrate navigation aspects around the unit and special notations that are used (e.g. Hyperlink notations that are used for definitions inside text).

Regarding the toolkit effectiveness and depth of coverage, the students expressed their opinion that the toolkit can help them improve and complete their security knowledge that is needed for their everyday exposure to information technology. The presentation and coverage of information security terms were adequate along with the examples used and the rationale on why information security is important.

Further to that, the students believed that the methods of choosing a good password along with its qualities were sufficiently presented, and the risks associated with using social networking sites were adequately covered.

As a final observation, it should be noted that a small percentage of students from both groups (2 out of 7 for both 1st year and senior year students) failed the post-assessment part for the "Human Aspects of Security unit. This is justifiable for the following reasons which also apply in the case of the administrative group presented in this chapter:

- Exposure to the whole toolkit was part of the focus group and time was limitations applied.
- Participants were exposed to the toolkit part only once and did not have the time to go through it for a second time or at their own pace.
- This small failure rate was marginal. Because of the testing and evaluation purpose of the toolkit, the number of questions at the post-assessment unit were limited to five making it rather easy to fail. At the same time, someone may consider the passing score (80%) as high. Both these aspects may be considered as contributors to this small failure percentage.

Despite this observation, the results from the users' exposure to the toolkit are considered successful.

The Administrative group toolkit assessment

The participants expressed their feeling that the toolkit can significantly contribute to raising the awareness level of employees and regulate their security behavior through a continuous learning process.

Since most participants expressed a neutral opinion concerning whether they possess sufficient information security knowledge to perform their duties, for that reason they were very positive about the idea of the toolkit as a method of enhancing their security competencies. Accepting the idea that the toolkit was rather a prototype model for supporting security awareness raising methods, this group's participants suggested that in its final and complete form, it could track not only which user logged in and went through it but also (through the mini quizzes at the end of each module) who has actually read and absorbed the material.

The participants felt that the toolkit was easy to use and presented in an efficient way and engaging way. The depth of coverage of the material was sufficient, and the post-assessment quizzes could easily be answered after toolkit completion.

More specifically the participants made the following observations concerning their exposure to the toolkit:

- Through the toolkit, they could better link it with the concepts of confidentiality, integrity, and availability and the examples associated with them.
- Participants expressed their concern that as more and more online services require the use of a strong password (with forced periodic renewal), it would be difficult to easily remember all of them, thus driving them to insecure practices (e.g. using the same password for many services). A valuable addition to the toolkit, linked to the proliferation of passwords, could be a module describing the use of password managers.
- The toolkit helped identify aspects and variations regarding social engineering and at the same time classify threats that they were already exposed (e.g. Spear phishing) without knowing the essence behind them.
- Concerning social networking, since most of the participants have young children, they felt that the presentation of such threats and safeguards was useful in their effort to mentor their children concerning safe online behavior.

The Educators group toolkit assessment

This group involved individuals from institutions of higher education that are somehow involved in the learning process (e.g. technology specialists, library staff, faculty, etc.). In total 340 participants were surveyed and 116 responses were received.

Concerning the effectiveness of the "Introduction to Information Security" unit, most the respondents considered the unit as a good basis for promoting information security awareness. Their responses ("Agree" or "Strongly Agree") ranged between 90% and 99%. Participants felt that the post assessment questions covered the material presented and could be easily answered if the toolkit material was sufficiently covered (97%).

When tabulating the results by job function, no significant differences are observed. The only variation that can be witnessed is that library staff has less "Strongly agree" answers when compared with the rest of the groups.

Concerning the effectiveness of the "Human Aspects of Security" unit, the participants felt that upon its completion, will have a good understanding of what constitutes a weak password and the rules to be followed when choosing a password (Responses of "Agree" and "Strongly Agree" were measured at 99% for both questions). In respect to social engineering, although percentages are high (89%), it seemed that the participants had expressed a small degree of concern over their understanding of the concept along with the terms associated with it. A similar concern had been observed in respect to the rules to be followed when visiting social networking sites (a 19% of the respondents reported that social networking security recommendations were not clear to them). When tabulating the results by job function, no significant differences are observed.

In respect to the usability of the toolkit (Figure 5), the majority of the respondents considered the application easy to use (98%). Information was arranged in a natural and logical order (97%) and presented in a clear and easy to understand way (97%). In general, participants were satisfied with the system which kept them engaged with content that is relevant to what is to be learned (90%). The only usability concern observed – although the percentage recorded (19%) is not significant – had to do with the appearance of the system regarding colors, graphics, screen layouts and the ease of recognition in respect of hyperlinks, linked graphics, and menus. Most of the participants consider the toolkit as useful for presenting basic everyday information security principles and would recommend it to others who want to familiarize themselves with such security principles. Overall, 92% of the participants are satisfied (agree or strongly agree) with the eLearning unit.

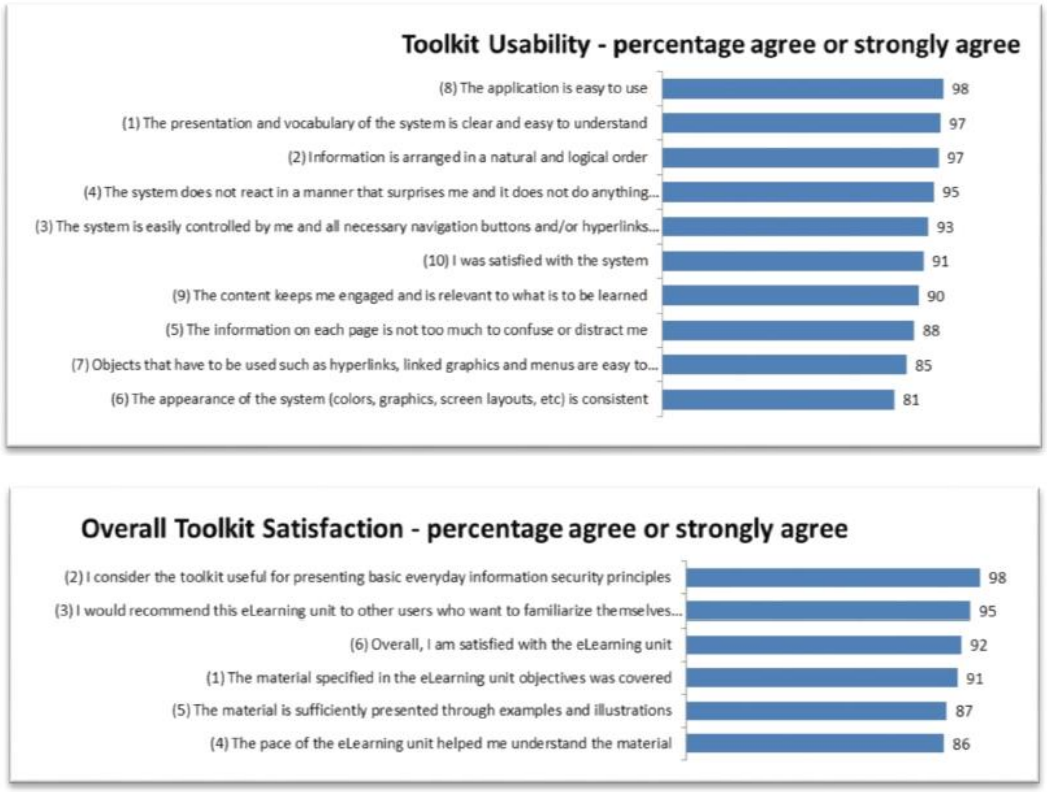


Figure 5: Educators Group Toolkit Usability and Overall Toolkit Satisfaction. Percentage agree or strongly agree

The IT Expert group toolkit assessment

The group included experts in the field, like people closely related to the IT function, IT managers/administrations and information security experts.

Regarding the survey responses collected, most the respondents who went through the first unit of the toolkit (Introduction to Information Security), either agree or strongly agree that this unit is a good basis for promoting information security awareness (Table 3). The results are rounded to whole number due to the small number of people that participated (14 in total). Very small variations that are recorded in a few questions are considered insignificant.

Survey Question	**Participant's answers**				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The learning area objectives are clear.	71%	29%	0%	0%	0%

The unit clearly describes why there is a need for Information Security Awareness.	79%	14%	7%	0%	0%
The definition of Information Security is clear along with its goals.	50%	50%	0%	0%	0%
The examples used to describe the goals of Information Security are easy to understand.	43%	57%	0%	0%	0%
The issues in respect to Information Security that affect users are clearly understood.	50%	50%	0%	0%	0%
The consequences of poor Information Security are clearly understood.	64%	29%	7%	0%	0%
The participant will gain a basic understanding of the Information Security terms and definitions.	36%	64%	0%	0%	0%
The different types of attackers along with their characteristics are clearly understood.	29%	64%	7%	0%	0%
The areas that need protection are clearly understood.	36%	57%	7%	0%	0%
I consider this unit as a good basis for promoting information security awareness.	71%	29%	0%	0%	0%
The quiz area questions reflect the material presented.	79%	21%	0%	0%	0%
The quiz area questions can be easily answered if the toolkit material is sufficiently covered.	64%	36%	0%	0%	0%

Table 3: IT Experts group, Introduction to Information Security unit. Participant responses.

Concerning the effectiveness of the "Human Aspects of Security" unit, the participants believed (Table 4) that the unit is a good basis for promoting information security awareness and the quiz questions presented at the end, can be easily answered from the material covered. The only variations by this testing group are recorded in the case of social networking sites. Although the opinions concerning the unit's coverage are not significant, most respondents feel that security recommendations concerning social networking sites and especially Facebook, may need some more attention and further revision. In the overall, the unit is considered a good basis for promoting information security awareness by most of the respondents.

Survey Question	**Participant's answers**				
	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
The examples that describe common human errors in respect to information security are clear.	57%	43%	0%	0%	0%
The importance of using passwords is clearly understood.	86%	14%	0%	0%	0%
The characteristics of a weak password are clearly understood.	64%	21%	14%	0%	0%
The rules a user has to follow when choosing a password are clear.	36%	64%	0%	0%	0%

The participant will understand how to test the strength and suitability of his chosen password.	71%	29%	0%	0%	0%
The participant will understand how to deal with passwords safely.	43%	57%	0%	0%	0%
The participant will understand what is meant when using the term “Social Engineering".	43%	50%	7%	0%	0%
The participant will gain a basic understanding of social engineering approaches and related terms.	36%	64%	0%	0%	0%
The participant will understand, what is a phishing attack, along with its variations.	57%	43%	0%	0%	0%
The participant will understand what is meant by the term ‘dumpster diving’.	57%	43%	0%	0%	0%
The participant will understand what is meant by the term ‘shoulder surfing’.	64%	36%	0%	0%	0%
The participant will gain a basic understanding of the techniques, a social engineer will use to obtain personal information.	71%	29%	0%	0%	0%
The participant will gain a basic understanding of the risks of visiting social networking sites.	29%	64%	7%	0%	0%
Facebook security recommendations are clear.	0%	21%	64%	14%	0%
The rules a user has to follow when visiting social networking sites are clear.	7%	79%	14%	0%	0%
The system has the appropriate topic coverage and depth from a security perspective.	21%	79%	0%	0%	0%
I consider this unit as a good basis for promoting information security awareness.	43%	57%	0%	0%	0%
The quiz area questions reflect the material presented.	71%	29%	0%	0%	0%
The quiz area questions can be easily answered if the toolkit material is sufficiently covered.	57%	43%	0%	0%	0%

Table 4: IT Experts group, Human Aspects of Security. Participant responses.

The main points concerning the toolkit usability as it is observed by this group can be summarized as follows:

- The whole unit uses a language that is easy to understand and can be used in a typical day-to-day environment addressed for novice users (93%).
- The flow of the system is natural, easily understood by a novice user without any confusion or unexpected system behavior.
- Information presented at each topic area is consistent without involving too much information that would confuse or distract the user (93%).
- In the overall, most the respondents of this group believe that the system is usable, has content that is relevant to what is to be learned and keeps the learner engaged.

The only areas of concern expressed by this group – although the number of responses is not significant – has to do with the with the appearance of the system regarding colors, graphics and screen layouts and the ease of recognition in respect of hyperlinks, linked graphics, and menus (21%). This opinion is in significance with what has been reported by the experts group previously, where a similar concern regarding the graphical richness of modern websites and Internet applications has been expressed.

The semi-structured interviews that followed, revealed similar results as the previously examined user groups. At the same time, this group believed that the toolkit could be further enhanced by taking into consideration the following:

- Include links to short documents, mainly in pdf format, where more detailed descriptions are provided for specific security issues already included in the toolkit pages, although this contains the risk of either not actually being visited or seriously considered by the user.
- Possibility to provide one additional option at the main screen of the toolkit (currently the existing options for each unit are “content” and “quiz”) called “demos” which will be solely dedicated to providing screen-by-screen demonstrations on security topics (e.g. step-by-step guide on how to change our password). It was felt that such an addition would add an extra level of friendliness to the toolkit by directing users on easy to understand everyday security steps.
- It might be helpful to subdivide each unit into smaller units and also give the participant to the opportunity to “jump” directly and complete this sub-unit at his own pace. For example, “Human Aspects of Security” could include its main title at the table of contents, giving the opportunity to the participant to cover the whole unit at once but also provide its distinct areas (e.g. Using passwords, understanding social engineering, dealing with social networking risks, etc.) as separate links for the participant to complete.

Finally, this group believed that the toolkit could be further utilized by taking into consideration the following suggestions:

- Be part of an overall employee orientation plan or as an important element of a new employee welcome "kit". Some companies as part of their recruitment process engage prospective employees in a series of tests (e.g. skills, character or psychological tests) and the inclusion of tests involving the security awareness of a future employee could be a useful addition.
- Be considered as part of an overall employee continuous education and development program where employees must go through periodically, refresh their knowledge and skills, and the completion and success level is used as an additional evaluation method for promotion and succession.
- Establish additional mechanisms where the effectiveness of the toolkit as an awareness raising method is continuously evaluated by measuring the resulting information security culture.

CONCLUSIONS & FUTURE WORK

This research study indicated the importance of protecting valuable information and an important aspect that must be addressed in this regard is information security awareness. It has to do with enabling all participants in the information security function to clearly understand the role they play and be aware of the rules and regulations they are expected to adhere to. The research identified the importance for addressing information security awareness along with its interdisciplinary nature. Although security awareness is an essential proactive measure to protect personal and organizational information systems through effective security practices, still there is a lot to be done to achieve an appropriate awareness level for the general population. Despite the existence of numerous online efforts addressed to different population groups, these efforts do not follow a clear and structured way (e.g. measure existing knowledge, present material where knowledge is lacking, assess knowledge gained) on how someone can be informed and prepared on various information security topics. Although they can be an excellent basis for security professionals entitled to create awareness materials, on the other hand, are not considered suitable for individuals that want to be informed and protected from potential threats.

To fill this gap, the research proposed the development of the "Information Security Toolkit". As an awareness-raising method, this addresses the general user population with the objective to establish the security knowledge and skills that all IT users need to acquire to be competent and confident users of technology.

Towards the development of the toolkit several learning theories are taken into consideration in order to create a piece that is user-friendly and at the same time achieves learning retention. Having in mind this challenge, the toolkit is created as a successful learning experience geared towards all generations by incorporating a variety of activities that utilize all learning styles.

Having developed a working prototype of the toolkit, the research was able to make an initial evaluation of its effectiveness. This was achieved by testing the toolkit using four representative groups of users, a group of students at different stages of their education cycle, a group of administrative staff, a group of experts involved in learning processes and a group of IT Experts. It is concluded that the security toolkit is a valuable resource to establish a sufficient level of security awareness amongst the online population.

The research can be further expanded and improved in the future by considering the following suggestions:

- A longer-term practical evaluation should be conducted to determine the effectiveness of the toolkit in raising awareness, as well as to enable refinement of the content and delivery styles.
- There is significant potential to further enhance the toolkit by including additional topics so from a working prototype it evolves to a complete set capable of assessing and establishing an appropriate level of awareness. Also, other related disciplines (e.g. interface designers, content creators, etc.) could further assist towards this effort.
- The security toolkit as an efficient awareness raising initiative could help towards achieving an appropriate level of security culture. There is a large potential for further research that will establish a holistic approach that continuously measures the resulting security culture and amends awareness efforts accordingly.

Students throughout their educational experiences (e.g. early education, high school, college and/or university) spent a significant time online. At the same time, the essential information security knowledge cannot be considered a fact. The research could form the basis for an appropriately developed information security curriculum across different educational levels and different educational disciplines. This could serve as the foundation for a security-aware society that not only understands the threats associated with information technology but also behaves in a security aware manner.

Information security is a widely accepted discipline since its value is recognized by everyone. So, all efforts towards security awareness should be continuous and updated to protect the online population. As their dependence seems likely to increase, the online population should be provided with the means that will help them not only appreciate the use of information technology but also understand the potential dangers associated with its use, so they behave in a secure way.

REFERENCES

Alessi, S. and Trollip, S. (2000). Multimedia for Learning: Methods and Development, Pearson.

Aloul, F. (2012). "The Need for Effective Information Security Awareness." Journal of Advances in Information Technology 3(3): 176-183.

Anderson, C. L. and R. Agarwal (2010). "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions." MIS Quarterly 34(3): 613-643.

Anttila, J., R. Savola, J. Kajava, J. Lindfors and J. Röning (2007). Fulfilling the Needs for Information Security Awareness and Learning in Information Society. 6th Annual Security Conference, Las Vegas, NV, Global Publishing, Washington DC, USA.

CEPIS (2014). "Assisting EU citizens with reliable ICT security information." Council of European Professional Informatics Societies. Retrieved February 27, 2014, from http://www.cepis.org/media/Assisting_EU_citizens_with_reliable_ICT_security_information 1.pdf.

Davis, P. (2008). "Measuring the Effectiveness of Information Security Awareness Training." Retrieved July 12, 2014, 2014, from http://www.saiglobal.com/Compliance/resources/WhitePapers/how-to-measure-information-security-training.htm.

ENISA (2007). Information Security Awareness initiatives: Current practice and the measurement of success, ENISA. July 2007.

ENISA (2010). The new Users' Guide: How to Raise Information Security Awareness, ENISA. November 2010.

Ernst & Young (2016). Path to cyber resilience: Sense, resist, react. EY's 19th Global Information Security Survey 2016-17. London, Ernst & Young.

Ernst & Young (2013). Under cyber attack. EY's Global Information Security Survey 2013. London, Ernst & Young.

European Travel Commission (2014). "Internet Usage Europe." Retrieved Aug. 1, 2014, from http://etc-digital.org/digital-trends/connectivity/internet-usage/regional-overview/europe/.

Forest, E. (2014, Jan. 29, 2014). "The ADDIE Model: Instructional Design." Retrieved April 18, 2014, from http://educationaltechnology.net/the-addie-model-instructional-design/.

Furnell, S., M. Gennatou and P. Dowland (2002). "A prototype tool for information security awareness and training." International Journal of Logistics Information Management 15(5): 352-357.

Herold, R. (2005). Managing and Information Security and Privacy Awareness and Training Program. Boca Raton, FL, Auerbach Publications.

International Organization for Standardization (ISO) (2013). ISO/IEC 27002, Information technology - Security Techniques - Code of practice for information security controls.

ITGI (2007). "COBIT Security Baseline: an information security survival kit." IT Governance Institute 2nd edition. from www.itgi.org.

Karjalainen, M., Siponen, M., Puhakainen, P., and Sarker, S. (2013). "One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions." PACIS 2013 Proceedings. Paper 98.

Kaspersky Lab (2013). "Global Corporate IT Security Risks: 2013." Retrieved July 1st, 2014, 2014, from http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf.

Korovessis, P. (2011). "Information Security Awareness in Academia." International Journal of Knowledge Society Research (IJKSR) 2(4): 1-17.

Kruger, H. and Kearney, W. (2006). "A prototype for assessing information security awareness." Computers & Security 25(4): 289-296.

Laberis B. (2016). "20 Eye-Opening Cybercrime Statistics." Security Intelligence-Analysis and Insight for Information Security Professionals. Retrieved April, April 2017, from https://securityintelligence.com/20-eye-opening-cybercrime-statistics/.

Lacey, D. (2009). Managing the human factor in Information Security. West Sussex, UK, John Wiley & Sons Inc.

Li, Y. and M. Siponen (2011). A call for research on home users' information security behaviour. Pacific Asia Conference on Information Systems, Brisbane, Australia.

McIlwraith, A. (2006). Information Security and Employee Behavior: how to reduce risk through employee education, training and awareness. Hampshire, UK, Gower Publishing Limited.

National Institute of Standards and Technology (NIST) (1998). "Information Technology Security Training Requirements: A Role- and Performance-Based Model, Special Publication 800-16." Retrieved September 3, 2007, from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

Nonaka, I. and Takeuchi, H. (1995). The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation, Oxford University Press, USA.

Olzak, T. (2006). "Strengthen Security with an Effective Security Awareness Program ". from http://adventuresinsecurity.com/Papers/Build_a_Security_Awareness_Program.pdf.

PWC (2016). "Global Economic Crime Survey 2016." Retrieved Apr. 08, 2017, from http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html.

Pew Research Center (2014). "The Web at 15." Retrieved Aug. 1, 2014, from http://www.pewinternet.org/files/2014/02/PIP_25th-anniversary-of-the-Web_0227141.pdf.

Puhakainen, P. and Siponen, M. (2010). "Improving employees' compliance through information systems security training: an action research study." MIS Q. 34(4): 757-778.

Symantec (2016). Internet Security Threat Report. Symantec Corporation. 21.

U.S. Department of Homeland Security (2017). "National Cyber Security Awareness Month." Retrieved Apr. 17, 2017, 2017, from https://www.dhs.gov/national-cyber-security-awareness-month.

Wilson Mark and Hash Joan (2003). "Building an Information Technology Security Awareness and Training Program, (NIST), Special Publication 800-50." Retrieved September 11, 2007, from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.